

REMARKS

Claims 4-12 are pending in this application. Claims 4-7 have been amended to address the Examiner's objections. New claims 8-12 have been added in this amendment. No new matter has been introduced. Favorable reconsideration is respectfully requested.

With regard to the IDS and Oath/Declaration, the Applicants acknowledge the Examiners comments and will provide the requested documents in due course.

Claims 1- 7 were rejected under 35 U.S.C. § 103(a) as being unpatentable over *Davis* (U.S. Patent 5,539,828) in view of *Rune* (U.S. Patent 5,850,444). Applicant respectfully traverses this rejection, because the cited reference, alone or in combination, do not disclose or suggest features of the present invention as described in independent claims 4 and 8.

The authentication of key devices in the present invention is based on a public-private key system. An administrator AD (i.e., the certification system) publishes a public key pAD that corresponds to the secret private key sAD of the administrator AD to all the key devices being member of the group of certified key devices. Additionally, in the certification phase, a key device A of the group of certified key devices is assigned a certificate Z(A) containing specific attributes of the key device (e.g., device name for identifying the key device A in the group of certified key devices, authenticating the key device A as being a member of the group of certified key devices, etc.). Furthermore, the key device A receives a signature S(Z(A)) from the administrator AD which is its encrypted certificate Z(A) encrypted by the secret private key sAD of the administrator AD.

If key device A transmits a message M to another key device B in the group of certified key devices, key device A encrypts M with the public key pAD and transmits the encrypted message M with its certificate Z(A) and its signature S(Z(A)) to the key device B.

The key device B decrypts the signature S(Z(A)) with the public key pAD received from the administrator AD. If the key device A is a member of the group of key devices certified by administrator AD, the decryption of the signature S(Z(A)) of key device A, performed by key device B, leads to the correct certificate Z(A) of key device A. The identity of the decrypted signature S(Z(A)) with the correct certificate Z(A) is evaluated by comparing the decrypted signature S(Z(A)) with the correct certificate Z(A) of key device A transmitted from key device A to key device B. The identity between the decrypted signature S(Z(A)) and the certificate

Z(A) of key device A is the prove for the correct authentication of key device A in the group of certified key devices. Therefore key device B can trust in the correct origin of the received message M as being a message of the certified key device A, and not being a manipulated message of a third party sender not being certified in the group of certified key devices.

The authentication of the hardware agents of the semiconductor devices in the group of certified semiconductor devices in *Davis* and the cited art is realized by a certification system. The certification system in *Davis* receives, in the certification phase, a pair of public and private keys from each hardware agent. By enlisting a different pair of public and private key for each hardware agent in a storage device of the certification system each hardware agent, can be identified by its specific pair of public and private keys. For authentication of each hardware agent, the certification system creates for each hardware agent a certificate by encrypting the public key of each hardware agent with its secret private key. Each hardware agent X; receives its specific certificate and stores it for authentication purpose (col. 5, line 66 to col. 6, line38).

Furthermore, the hardware agent sends *only the certificate* to the remote system for its authentication when communicating with a remote system (col. 4, lines 23-39). The remote system decrypts the certificate with the public key received from the certification system and thus obtains the public key of the hardware agent. The remote system is not able to derive the authentication of the hardware agent, from the information of the public key, because it has not any information about all the members of the group of certified hardware agents. Therefore, the remote system sends a test data back to the hardware agent. The hardware agent answers by encrypting the test data with its secret private key, and resending the encrypted test data to the remote system. The remote system decrypts the encrypted test data received from hardware agent with the public key, determined by decrypting the certificate of the hardware agent, if the decrypted test data complies with the sent test data. The public key is determined by decrypting the certificate of the hardware agent, which corresponds to the private key used by the hardware agent for encrypting the received test data. This provides verification that the hardware agent - the communication partner of the remote system - is a certified member of the group of certified semiconductor devices and the authentication of the hardware agent, is guaranteed.

In contrast, the present invention authenticates in three steps for identifying the device by means of device-specific information, authenticating the device by means of a group-specific

information, and achieving compliance between the identified and the authenticated device which were performed by the communication partner of the device. In the present invention, the key device B identifies the key device A by receiving the certificate $Z(A)$ from the key device A, which is a device-specific information characterizing the identity of key device A. The key device B authenticates the key device A (i.e., determines the membership of key device A to the group of certified key devices) by decrypting the signature $S(Z(A))$ (i.e., the device-specific information about the membership of key device A to the group of certified key devices) by means of the public key pAD (i.e. the group-specific information). The key device B achieves compliance between the identified and the authenticated devices by comparing the received certificate $Z(A)$ (i.e., the identity characterizing information of the key device A) with the certificate $Z(A)$ derived from the signature $S(Z(A))$ (i.e., the authentication characterizing information of the device A to the group of certified key devices) by means of the group-specific information public key pAD.

In the cited art, there is a lack of assured information about the identity of the hardware agent in the authentication process performed by the remote system. Therefore the remote system has to perform an additional data communication -i.e. sending test data to the hardware agent and receiving encrypted test data from the hardware agent, thereby complicating the authentication process in comparison with the present invention.

As mentioned above, the present invention solves this problem by transmitting a corresponding device-specific certificate $Z(A)$ -i.e. the identity characterizing information of key device A - and a corresponding device-specific signature -i.e. an authentication characterizing information of key device A - to another one of the key devices -i.e. for example key device B.

In light of the above, Applicant respectfully submits that claims 1-15 are now in condition for allowance, which is respectfully requested.

Respectfully submitted,

BELL, BOYD & LLOYD LLC

BY


Peter Zura

Reg. No. 48,196

Bell, Boyd & Lloyd LLC

P.O. Box 1135

Chicago, Illinois 60690-1135

Phone: (312) 807-4208

Dated: May 27, 2004